R E P U B L I Q U E F R A N C A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

PCT/FR 0 0 / 0 1 0 4 7

REC'D 2 2 MAY 2000
WIPO PCT

GJU

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 27 AVR. 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ
PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.A) OU B))

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 20 AVR 1999

N° D'ENREGISTREMENT NATIONAL 99 04975

DÉPARTEMENT DE DÉPÔT 75

DATE DE DÉPÔT 20 AVR. 1999

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

BULL S.A.
Monsieur Bernard CORLU / PC 58F35
68, route de Versailles
78434 LOUVECIENNES CEDEX

n°du pouvoir permanent PG 4280 références du correspondant FR3797/BC téléphone 01 39.66.61.76

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ▷ demande initiale ◁

☐ certificat d'utilité ☐ transformation d'une demande de brevet européen ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

Procédé de vérification de signature ou d'authentification.

3 DEMANDEUR (S) n° SIREN 3 2 9 5 5 6 1 4 6 code APE-NAF B 3 2 1

Nom et prénoms (souligner le nom patronymique) ou dénomination

BULL CP8

Forme juridique

S.A.

Nationalité (s) Française

Adresse (s) complète (s) Pays

BULL CP8
BP 45
68, route de Versailles
78430 LOUVECIENNES

FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt : joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine | numéro | date de dépôt | nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

Bernard CORLU
Mandataire -

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

BA 540 A/200296

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53.04 - Télécopie : 01 42 93 59 30

FR 3797/BC

N° D'ENREGISTREMENT NATIONAL

9504975

TITRE DE L'INVENTION :

Procédé de vérification de signature ou d'authentification.

LE(S) SOUSSIGNÉ(S)

BULL S.A.

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

Goubin Louis
3 rue Brown Séquard
75015 PARIS
France

Patarin Jacques
11 rue Amédée Dailly
78220 VIROFLAY
France

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Louveciennes, le 16 avril 1999

Corlu Bernard (mandataire)

BA 113/140897

Procédé de vérification de signature ou d'authentification

La présente invention concerne un procédé permettant de rendre plus efficace, en temps de calcul, en RAM et ROM nécessaires, la vérification d'une signature ou d'une authentification asymétrique requérant quelques multiplications modulo n ou des grands nombres.
Les algorithmes de signature ou d'authentification RSA et Rabin sont des exemples permettant la mise en œuvre de ce procédé.

Le procédé est plus particulièrement adapté en vue d'une mise en œuvre dans le cas où un ordinateur, par exemple un ordinateur personnel désigné par PC, qui génère une signature ou une authentification au moyen d'une clé secrète qui doit ensuite être vérifiée par une carte à microcalculateur. Le microcalculateur effectue cette vérification au moyen d'une clé publique. Il dispose de relativement peu de puissance en comparaison du PC.

Par "*carte à microcalculateur*", on entend un microcontrôleur monolithique standard, avec mémoire incorporée.

Actuellement la majorité des algorithmes à clé publique utilisés dans le monde effectuent des calculs modulo de "*grands nombres*". Par "*grands nombres*", on désigne des nombres entiers positifs et d'au moins 320 bits. Pour des raisons de sécurité, la communauté scientifique recommande même actuellement d'utiliser des nombres d'au moins 512 bits, voire 1024 bits pour la plupart des algorithmes, par exemple pour les algorithmes RSA ou Rabin.

Actuellement les cartes à microcalculateur sont amenées à dialoguer avec des ordinateurs ayant des

capacités de calcul bien plus importantes qu'elles-mêmes. De plus, pour des raisons de coût, on utilise souvent des cartes à microcalculateur sans coprocesseur arithmétique, et avec des ressources en mémoire (ROM, RAM et EEPROM) très limitées. De ce fait, les calculs normalement requis pour réaliser une vérification d'authentification, ou une vérification de signature à clé publique, utilisant des calculs modulo de grands nombres sont souvent très longs, voire impossible faute de mémoire suffisante, si l'on utilise les descriptions traditionnelles des algorithmes cryptographiques.

Dans la suite de la description on désigne par :

- "*prouveur*" : l'entité qui veut être authentifiée, ou qui produit une signature. Elle effectue pour cela des calculs faisant intervenir la clé secrète de l'algorithme asymétrique utilisé. Il s'agira par exemple d'un ordinateur de type PC.
- "*vérifieur*" : l'entité qui vérifie l'authentification, ou qui vérifie la validité d'une signature. Elle effectue pour cela des calculs faisant intervenir uniquement la clé publique de l'algorithme cryptographique asymétrique utilisé. Il s'agira par exemple d'une carte à microcalculateur.

La présente invention a pour objet la mise en œuvre d'un procédé de vérification de signature et d'authentification permettant de remédier aux inconvénients précités inhérents à la capacité de calcul plus limitée d'une entité vérifieur, constituée par une carte à microcalculateur, vis-à-vis d'une entité prouveur, tel qu'un ordinateur personnel ou autre muni d'un dispositif lecteur de carte.

Un autre objet de la présente invention est en conséquence une simplification des opérations de calcul de

certaines réductions modulaires du vérifieur grâce à la mise en œuvre de calculs supplémentaires du prouveur, la tâche du vérifieur étant ainsi simplifiée en l'absence de tout affaiblissement de la sécurité théorique de l'ensemble.

Le procédé de vérification de signature respectivement d'authentification au moyen d'un processus de calcul cryptographique asymétrique à clé privée et à clé publique, objet de la présente invention, ce procédé étant conduit entre une entité *"prouveur"* et une entité *"vérifieur"*, l'entité prouveur effectuant des calculs cryptographiques à partir de la clé privée en vue d'effectuer un calcul de signature, respectivement une valeur d'authentification, et l'entité vérifieur à partir de cette valeur transmise effectuant des calculs cryptographiques à partir de cette clé publique en vue de procéder à cette vérification de signature, respectivement à cette authentification, les opérations de calcul cryptographique mettant en œuvre le calcul de multiplications modulo n ou des grands nombres, est remarquable en ce que, pour un processus de calcul cryptographique mettant en œuvre une clé publique, constituée par un exposant public e et un modulo public n, et une clé privée constituée par un exposant privé, d, ce procédé consiste à calculer, au niveau de l'entité prouveur, au moins une valeur de prévalidation et à transmettre de l'entité prouveur à l'entité vérifieur cette au moins une valeur de prévalidation, permettant à l'entité vérifieur d'effectuer au moins une réduction modulaire en l'absence de toute opération de division pour cette réduction modulaire.

Le procédé, objet de la présente invention, s'applique dans le cadre de tout dialogue ou protocole

d'échange de messages entre une entité prouveur telle qu'un ordinateur personnel et une entité vérifieur telle qu'une carte à microcalculateur, en particulier dans le cadre de transactions bancaires, de contrôle d'accès ou analogue.

Il sera mieux compris à la lecture de la description ci-après et à l'observation des dessins dans lesquels :

- la figure 1 représente un schéma illustratif du procédé, objet de la présente invention, mis en œuvre entre une entité prouveur et une entité vérifieur ;

- la figure 2a représente un schéma illustratif du procédé, objet de la présente invention, mis en œuvre à partir d'un algorithme de Rabin en vérification d'authentification ;

- la figure 2b représente un schéma illustratif du procédé, objet de la présente invention, mis en œuvre à partir d'un algorithme de Rabin en vérification de signature ;

- la figure 3a représente un schéma illustratif du procédé, objet de la présente invention, mis en œuvre à partir d'un algorithme RSA en vérification d'authentification ;

- la figure 3b représente un schéma illustratif du procédé, objet de la présente invention, mis en œuvre à partir d'un algorithme RSA en vérification de signature.

Une description plus détaillée du procédé, objet de l'invention, sera donnée en liaison avec la figure 1 et les figures suivantes.

Le procédé objet de l'invention met en œuvre, au niveau de l'entité vérifieur, des algorithmes à clé publique requérant des multiplications modulo n, ou des grands nombres, et les modifie légèrement en faisant faire

le calcul d'un ou de plusieurs quotients q à l'extérieur, c'est-à-dire au niveau de l'entité prouveur, et en fournissant ce ou ces quotients au vérifieur. Ainsi le vérifieur peut plus facilement et plus rapidement calculer certaines multiplications modulaires : au lieu de calculer a*b modulo n, il aura juste à calculer a*b, q*n, et a*b-q*n, a, b désignant des valeurs des calcul de vérification de signature ou d'authentification. Parfois, pour la sécurité il utilise cette dernière valeur d'une façon qui lui permettra de s'assurer que cette dernière valeur est bien comprise entre 1 et n. Lorsque l'on modifie ainsi un algorithme, en "*précalculant*" donc certains quotients, qui sont fournis au vérifieur afin de simplifier les calculs exécutés par ce dernier, on parle d'algorithme "*sous-jacent*" pour désigner l'algorithme initial dont on est parti, avant de faire cette modification. Ainsi, en référence à la figure 1, conformément à un aspect remarquable du procédé objet de la présente invention, le ou les quotients q, vérifiant la relation q=a*b/n, constituent une ou plusieurs valeurs de prévalidation transmises à l'entité vérifieur afin de permettre à l'entité vérifieur d'effectuer au moins une réduction modulaire en l'absence de toute opération de division pour cette réduction modulaire. En référence à la figure 1, on indique que le procédé objet de l'invention peut être mis en œuvre soit en vérification de l'authentification, suite à l'envoi 0 d'une valeur d'incitation tel qu'un aléa a, calcul 1 en interne au niveau du prouveur d'une valeur de réponse $b = a^d \bmod n$, et de la valeur de prévalidation q, transmission 2 de b et q du prouveur au vérifieur et calcul 3 par le vérifieur des quantités a*b, q*n et a*b-q*n pour procéder à la vérification de l'authentification, soit à la vérification

de signature d'un message M, suite au calcul 1 au niveau du prouveur d'une signature $S = S_d(M)$ du message M et de la valeur de prévalidation q, envoi 2 du vérifieur au prouveur de q, S et M, calcul 3 au niveau du vérifieur des quantités $a*b = S*S$, $q*n$ et $a*b-q*n$ pour procéder à la vérification de signature.

Dans la figure 1 et les figures suivantes, une flèche droite représente la transmission des valeurs précitées entre vérifieur et prouveur ou réciproquement et une boucle fléchée au niveau du prouveur ou du vérifieur représente la mise en œuvre d'un calcul interne au niveau du prouveur ou du vérifieur. Enfin, dans la suite de la description, on désigne par réponse R soit la valeur calculée b par chiffrement de l'aléa a dans le cas d'une vérification d'authentification $b = a^d \bmod n$, soit la valeur de signature $S = S_d(M)$ suite à la mise en présence du vérifieur et du prouveur.

Différents exemples de mise en œuvre du procédé objet de la présente invention seront maintenant décrits à partir des algorithmes sous-jacents, désignés par algorithmes RSA et algorithmes de Rabin.

Algorithmes RSA et de Rabin sous-jacents

L'algorithme RSA est le plus célèbre des algorithmes cryptographiques asymétriques. Il a été inventé par RIVEST, SHAMIR et ADLEMAN en 1978. On peut le trouver décrit dans :

R.L. RIVEST, A. SHAMIR, L.M. ADLEMAN : A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, 21, n°2, 1978, pp. 120-126.

ou dans les documents suivants :

- ISO/IEC 9594-8/ITU-T X.509, Information Technology - Open Systems Interconnection - The Directory: Authentication Framework ;

- ANSI X9.31-1, American National Standard, Public-Key Cryptography Using Reversible Algorithms for the Financial Services Industry, 1993.

Ces documents sont introduits dans la présente description à titre de référence.

L'algorithme RSA utilise un nombre entier n qui est le produit de deux grands nombres premiers p et r, et un nombre entier e, premier avec ppcm(p-1,r-1), et tel que $e \neq \pm 1$ modulo ppcm(p-1,r-1). Les entiers n et e constituent la clé publique. Le calcul en clé publique fait appel à la fonction α de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ définie par $\alpha(x)=x^e \bmod n$. Le calcul en clé secrète fait appel à la fonction $\alpha^{-1}(y)=y^d \bmod n$, où d est l'exposant secret, appelé aussi *"clé secrète"* ou *"clé privée"*, défini par $ed \equiv 1 \bmod ppcm(p-1,r-1)$.

Notons n le modulo public RSA, notons d l'exposant secret RSA et notons e l'exposant public RSA.

Dans le cas d'une vérification d'authentification, le vérifieur génère un nombre aléatoire A modulo n, et l'envoie au prouveur. Celui ci calcule alors $B= A^d$ modulo n, et renvoie cette valeur B au vérifieur. Celui-ci accepte alors l'authentification si et seulement si: B^e modulo n = A.

La plus petite valeur de e pour mettre en œuvre l'algorithme RSA est e = 3. Pour e = 2, on parle d'algorithme de Rabin ; celui-ci sera décrit ci-après dans la description. Cette valeur e = 3 est intéressante car elle permet au vérifieur de n'avoir à effectuer que deux multiplications modulaires.

L'algorithme de Rabin est en quelque sorte un algorithme RSA avec l'exposant public e = 2. En fait, lorsque e = 2, la fonction x^e n'est pas bijective

modulo n, lorsque n est le produit de deux nombres premiers > 2, on introduit donc des petites modifications dans l'utilisation de l'algorithme de Rabin par rapport au RSA.

On peut trouver une description de l'algorithme de Rabin dans :

M.O. Rabin, Digitized Signatures and Public-Key Functions as intractable as Factorization, Technical Report LCS/TR-212, M.I.T. Laboratory for Computer Science, 1979, introduit dans la présente demande de brevet à titre de référence.

Exemples de mise en œuvre du procédé objet de l'invention à partir des algorithmes de Rabin et RSA

◆ Algorithme de Rabin

Le procédé, objet de la présente invention, sera tout d'abord décrit dans un mode de réalisation particulier non limitatif à partir de l'algorithme de Rabin, soit pour e = 2.

◆◆ Vérification d'authentification

Ainsi que représenté en figure 2a, un exemple possible d'utilisation de l'algorithme de Rabin en vérification d'authentification est maintenant décrit.

Notons n le modulo public. Le vérifieur génère un nombre aléatoire A modulo n, et l'envoie, 0, au prouveur. Celui-ci calcule alors un nombre B, et renvoie, 1, cette valeur B au vérifieur. Celui-ci accepte alors l'authentification si et seulement si: B*B modulo n est égal à l'une des quatre valeurs possibles suivantes : A, ou n-A, ou C*A modulo n, ou -C*A modulo n. C est un nombre fixé par le protocole, C = 2 le plus souvent.

Pour simplifier le processus de vérification, conformément au procédé objet de la présente invention, le prouveur n'envoie pas, en 2, la valeur B seule : il envoie

B et Q, où Q est le quotient de B*B par le modulo public n. Le vérifieur vérifie alors que D_{AR} = B*B - Q*n est bien égal à l'une des quatre valeurs suivantes : A, n-A, (C*A) modulo n, ou (-C*A) modulo n. De plus, il peut calculer (C*A) modulo n en calculant C*A, en gardant cette valeur si elle est < n, et en prenant la valeur C*A - n sinon. De même, il peut calculer (-C*A) modulo n en calculant n-C*A, en gardant cette valeur si elle est >= 0, et en prenant la valeur C*n - C*A sinon. Ainsi le vérifieur n'a plus aucune division à effectuer.

◆◆ Vérification de signature

Ainsi que représenté en figure 2b, et en conservant les mêmes notations que ci-dessus, on note M le message dont le vérifieur souhaite vérifier la signature S. La signature S est obtenue à partir de la clé privée d par S = $S_d(M)$, $S_d(M)$ désignant l'opération de calcul de signature du message M. Si S est une signature Rabin de M, alors le vérifieur vérifie normalement que S*S modulo n = f(M) ou n-f(M), ou (2*f(M) modulo n) ou (-2*f(M) modulo n), où f est une fonction publique standardisée du message M. Par exemple f est la fonction identité, ou bien est décrite dans une norme de signature ; par exemple on peut utiliser les opérations de *paddage* ou concaténation de la norme PKCS#1, établie pour du RSA normalement, confer les éléments descriptifs de cette norme ci-après dans la description.

En conservant les mêmes notations que ci-dessus, pour simplifier le processus de vérification de la signature, ainsi que représenté en figure 2b, dans le procédé objet de la présente invention, le prouveur n'envoie pas, en 2, la valeur S seule : il envoie S et Q, où Q est le quotient de S*S par le modulo public n. Le vérifieur vérifie alors que D_{SR} = S*S - Q*n est bien égal

à f(M), ou n-f(M), ou C*f(M) modulo n, ou -C*f(M) modulo n, où C est un nombre fixé par le protocole, C pouvant être pris égal à 2. Comme ces deux dernières valeurs peuvent être calculées modulo n en effectuant zéro ou une soustraction par n, le vérifieur n'a plus aucune division à calculer.

◆ Algorithme RSA

Le procédé, objet de la présente invention, sera maintenant décrit dans un mode de réalisation particulier non limitatif à partir de l'algorithme RSA, soit pour e = 3.

◆◆ Vérification d'authentification

Ainsi que représenté en figure 3a, à partir d'un aléa A, pour simplifier le processus de vérification, dans la présente invention le prouveur n'envoie pas, en 2, la valeur B seule : il envoie B, Q1 et Q2, où Q1 est le quotient de B*B par le modulo public n, et où Q2 est le quotient de B*(B*B - Q1*n) par n. Le vérifieur vérifiera alors que D_{ARSA} = B*(B*B - Q1*n) -Q2*n est bien égal à A. Ainsi le vérifieur n'a plus aucune division à effectuer.

◆◆ Vérification de signature

En conservant les mêmes notations que ci-dessus et en notant M le message dont le vérifieur souhaite vérifier la signature S, S est une signature RSA de M, alors le vérifieur vérifie normalement que S^e modulo n = f(M), où f est une fonction publique standardisée du message M. Par exemple f est la fonction identité, ou bien est décrite dans une norme de signature RSA, comme par exemple la norme PKCS#1. La fonction publique normalisée peut consister à appliquer au message M une fonction de condensation SHA-1 pour obtenir un condensé de message CM, puis à concaténer à ce condensé de message une valeur constante.

Ainsi que représenté en figure 3b, et en conservant les mêmes notations que ci-dessus, pour simplifier le processus de vérification de la signature, dans le procédé, objet de la présente invention, le prouveur n'envoie pas, en 2, la valeur S seule : il envoie S, Q1 et Q2, où Q1 est le quotient de S*S par le modulo public n, et où Q2 est le quotient de S*(S*S - Q1*n) par n. Le vérifieur vérifiera alors que D_{SRSA} = S*(S*S - Q1*n) -Q2*n est bien égal à f(M). Ainsi le vérifieur n'a plus aucune division à effectuer.

La fonction de condensation SHA-1 est une fonction publique de "*condensation*". Elle prend en entrée un message dont la taille peut aller de 0 octets à plusieurs Giga octets, et donne en sortie un "*condensé*" du message de 160 bits. Cette fonction est souvent utilisée dans des normes ou avec des algorithmes de signature, car elle est réputée être résistante aux collisions, c'est-à-dire que l'on ne sait pas trouver concrètement deux messages distincts qui ont le même condensé (il en existe mais on ne sait pas comment trouver un tel couple de messages). Ceci permet de signer le condensé des messages plutôt que les messages eux-mêmes.

La norme PKCS#1 est une norme de signature RSA. Elle décrit une fonction publique f. Cette fonction f est appliquée sur le message M à signer avec RSA avant de lancer l'opération d'exponentiation modulaire RSA proprement dite : la signature RSA de M sera donc S = $(f(M))^d$ modulo n, où n est le modulo public RSA et où d est l'exposant secret RSA. f utilise une fonction de condensation (par exemple SHA-1) suivie d'un *paddage*, ou concaténation, avec une constante.

Pour une description plus détaillée, on peut consulter : PKCS#1, RSA *Encryption Standard*, version 2, 1998, disponible à l'adresse suivante :
ftp://ftp.rsa.com/pub/pkcs/doc/pkcs-1v2.doc
dont la version éditée est introduite dans la présente demande à titre de référence.

L'invention consiste ainsi à fournir des données supplémentaires au vérifieur afin de lui faciliter les calculs. Pour précalculer ces données, ici des quotients constituant la ou les valeurs de pré-validation, on n'a pas besoin d'utiliser la clé secrète de l'algorithme. Cela signifie que ces données sont complètement redondantes par rapport aux valeurs transmises à la carte dans une utilisation "*classique*" de l'algorithme asymétrique. En fait, dans la version "classique", la carte sait retrouver elle-même ces quotients. Il n'y a donc aucune information supplémentaire fournie à la carte, au sens de la théorie de l'information, lorsqu'on met en œuvre le procédé, objet de la présente invention tel que décrit précédemment. Cela montre que la sécurité de l'ensemble n'est en rien affaiblie par rapport à la mise en œuvre "*classique*" de l'algorithme.

REVENDICATIONS

1. Procédé de vérification de signature respectivement d'authentification au moyen d'un processus de calcul cryptographique asymétrique à clé privée et à clé publique, entre une entité *"prouveur"* et une entité *"vérifieur"*, l'entité prouveur effectuant des calculs cryptographiques à partir de ladite clé privée en vue d'effectuer un calcul de signature respectivement d'une valeur d'authentification constituant une valeur de réponse et l'entité vérifieur, à partir de cette valeur de réponse, effectuant des calculs cryptographiques à partir de ladite clé publique en vue de procéder à cette vérification de signature respectivement cette authentification, les opérations de calcul cryptographique mettant en œuvre le calcul de multiplications modulo n ou des grands nombres, caractérisé en ce que pour un processus de calcul cryptographique mettant en œuvre une clé publique, constituée par un exposant public e et un modulo public n, et une clé privée constituée par un exposant privé, celui-ci consiste :

- à calculer au niveau de ladite entité prouveur au moins une valeur de pré-validation ;

- à transmettre de l'entité prouveur à l'entité vérifieur ladite au moins une valeur de pré-validation, cette valeur de pré-validation permettant à l'entité vérifieur d'effectuer au moins une réduction modulaire en l'absence de toute opération de division pour cette réduction modulaire.

2. Procédé selon la revendication 1, caractérisé en ce que pour un exposant public e=2, le processus de calcul cryptographique étant basé sur un algorithme de RABIN, ladite au moins une valeur de pré-validation est constituée par une valeur unique, quotient Q du carré de

ladite valeur de signature respectivement de réponse par ledit modulo public n, $Q = R*R/n$, où R désigne ladite valeur de signature de réponse à une authentification.

3. Procédé selon la revendication 2, caractérisé en ce que suite à la réception par ladite entité vérifieur de ladite valeur de réponse à une vérification d'authentification respectivement de signature d'un message (M) et de ladite au moins une valeur de pré-validation, constituée par ledit quotient, ce procédé consiste, au niveau de ladite entité vérifieur :

- à calculer la différence (D_{AR}, D_{SR}) entre le carré de la valeur de réponse R*R et le produit Q*n dudit quotient Q par ledit modulo public n, (D_{AR}, D_{SR}) = $R*R - Q*n$;

- à vérifier l'égalité de ladite différence avec la valeur d'une fonction de cette valeur de réponse, en l'absence de toute opération de division par l'opération modulo n.

4. Procédé selon la revendication 1, caractérisé en ce que pour un exposant public e = 3, le processus de calcul cryptographique étant basé sur un algorithme RSA, ladite au moins une valeur de pré-validation est constituée par :

- un premier quotient Q_1 du carré R*R de ladite valeur de réponse R par ledit modulo public n ;

- un deuxième quotient Q_2 du produit de ladite valeur de réponse et de la différence entre le carré R*R de cette valeur de réponse et du produit dudit premier quotient Q_1 et du modulo public n par ledit modulo public n, $Q_2 = R*(R*R - Q_1*n)/n$.

5. Procédé selon la revendication 4, caractérisé en ce que suite à la réception de ladite valeur de réponse R et de ladite au moins une valeur de pré-validation

constituée par lesdits premier et deuxième quotients Q_1, Q_2, ledit procédé consiste, au niveau de ladite entité vérifieur :

- à calculer la différence (D_{ARSA}, D_{SRSA}) entre le produit de ladite valeur de réponse R et de la différence entre le carré R*R de cette valeur de réponse et le produit dudit premier quotient Q_1 et du modulo public n et le produit dudit deuxième quotient Q_2 et dudit modulo public n, (D_{ARSA}, D_{SRSA}) = $R*(R*R - Q_1*n)-Q_2*n$;
- à vérifier l'égalité de cette différence avec la valeur d'une fonction de ladite valeur de réponse, en l'absence de toute opération de division par opération modulo n.

6. Procédé selon la revendication 3 ou 5, caractérisé en ce que pour une opération de vérification de signature d'un message (M), ladite fonction est une fonction publique normalisée f(M) de ce message M et consiste :

- à appliquer à ce message une fonction de condensation pour obtenir un condensé de message CM ;
- à concaténer à ce condensé de message une valeur constante.

7. Procédé selon l'une des revendications 3 ou 5, caractérisé en ce que pour une opération de vérification d'authentification, ce procédé consiste en outre à transmettre de l'entité vérifieur à l'entité prouveur une valeur d'incitation.

8. Procédé selon la revendication 7, caractérisé en ce que ladite valeur d'incitation est constituée par une valeur aléatoire A modulo n, ladite valeur de réponse R est constituée par une valeur chiffrée B, ladite fonction de la valeur de réponse est une fonction f(A) de ladite valeur aléatoire A.

9. Procédé selon l'une des revendications 3 et 7, caractérisé en ce que ladite fonction f(A) de ladite valeur aléatoire A est une fonction parmi les fonctions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

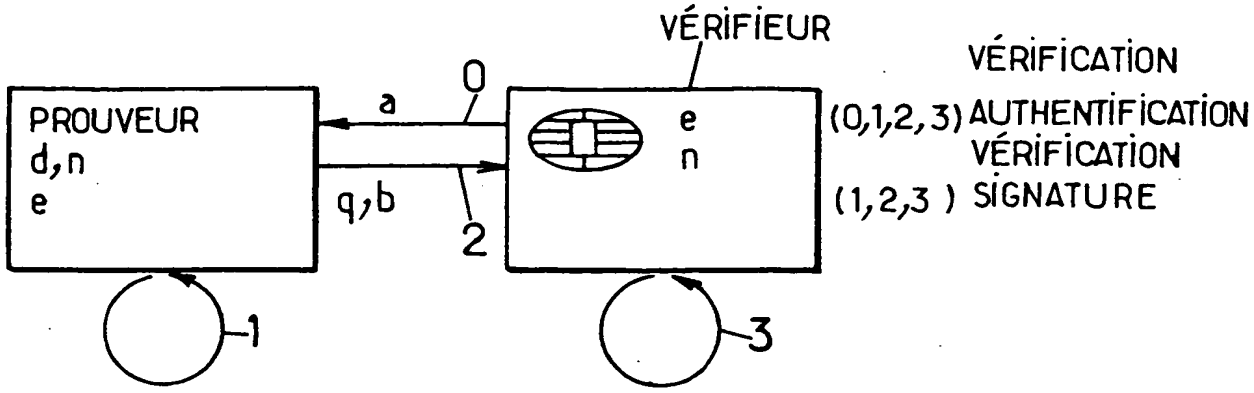
10. Procédé selon la revendication 9, caractérisé en ce que, au niveau de l'entité vérifieur, le calcul de ladite fonction f(A) = C*A modulo n est effectué par calcul de la valeur C*A et mémorisation de cette valeur si C*A < n et par calcul et mémorisation de la valeur C*A-n sinon, et en ce que le calcul de ladite fonction f(A) = -C*A modulo n est effectué par calcul de la valeur -C*A et mémorisation de cette valeur si -C*A < n et par calcul de la valeur intermédiaire n-C*A, et, si cette valeur intermédiaire est supérieure ou égale à zéro, calcul et mémorisation de la valeur de C*n-C*a comme valeur affectée à la valeur de -C*A modulo n sinon, ce qui permet de vérifier l'égalité de ladite authentification en l'absence de toute division pour réduction modulaire.

11. Procédé selon les revendications 5 et 8, caractérisé en ce que ladite fonction f(A) de ladite valeur aléatoire A est la fonction f(A) = A, ce qui permet de vérifier l'égalité de ladite différence et la validité de ladite authentification, en l'absence d'opération de division pour réduction modulaire.

12. Procédé selon les revendications 1, 2, 3 et 8, caractérisé en ce que ladite valeur de réponse, valeur chiffrée B, et ladite valeur de quotient Q sont concaténées préalablement à leur transmission de l'entité prouveur à l'entité vérifieur.

13. Utilisation du procédé selon l'une des revendications 1 à 12, l'entité vérifieur étant constituée

par un système embarqué tel qu'une carte à microprocesseur et l'entité prouveur par un système lecteur de carte.



$q = a * b / n$

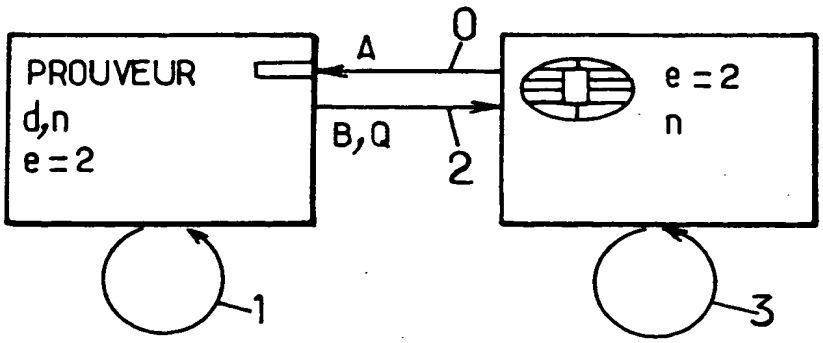
$b = \begin{cases} a^d \bmod n & \text{si } (0,1,2,3) \\ S = Sd(M) & \text{si } (1,2,3) \end{cases}$

$a * b$

$q * n$

$a * b - q * n$

FIG.1.



$R = B = A^d \bmod n$

$Q = B * B / n$

$D_{AR} = B * B - Q * n$

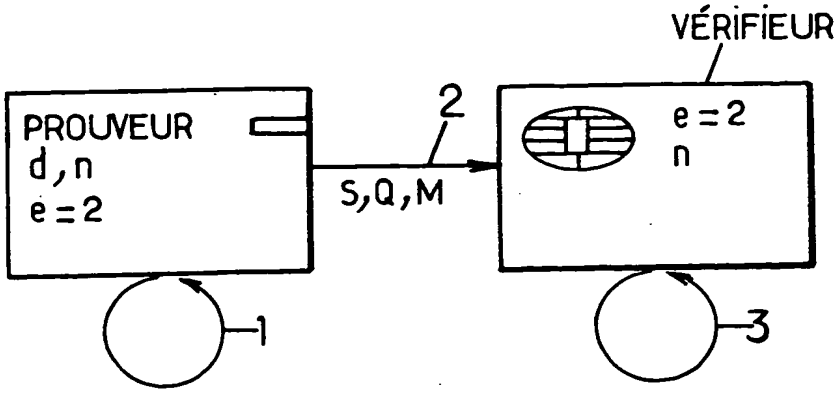
$D_{AR} = A$

$D_{AR} = n - A$

$D_{AR} = C * A \bmod n = C * A$ si $C * A < n$

$D_{AR} = -C * A \bmod n = C * A - n$ SINON

FIG. 2a.



VÉRIFICATION SIGNATURE

$R = S = Sd(M)$

$Q = S * S / n$

$D_{SR} = S * S - Q * n$

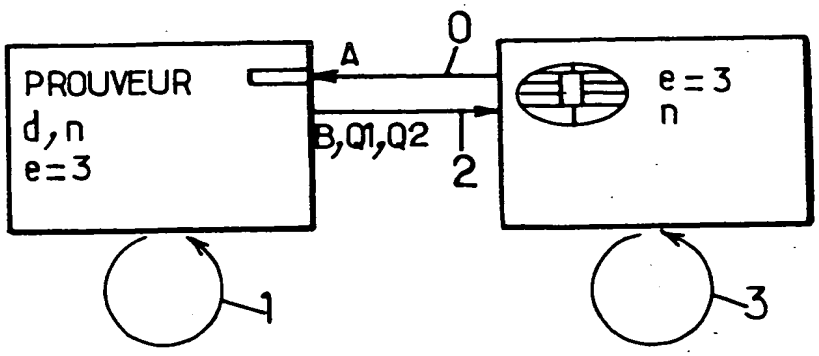
$D_{SR} = f(M)$

$= n - f(M)$

$= C * f(M) \bmod n = C * f(M)$ Si $< n$

$= C * f(M) \bmod n = C * f(M)$ SINON

FIG.2b.



VÉRIFICATION D'AUTHENTIFICATION

$R = B = A^d \bmod n$

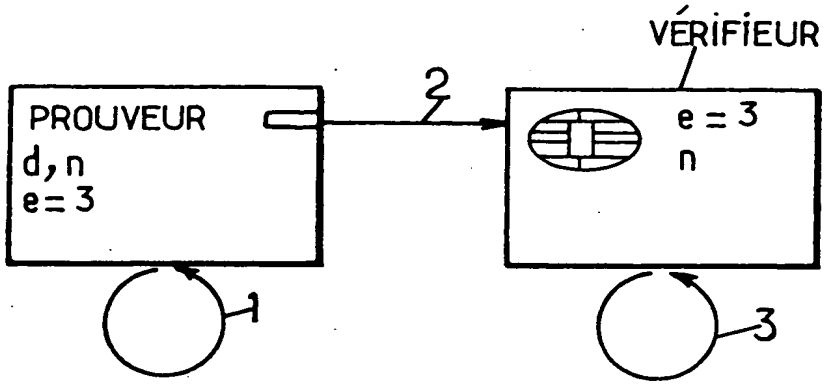
$Q1 = B * B / n$

$Q2 = B(B * B - Q1 * n) / n$

$D_{ARSA} = B(B * B - Q1 * n) - Q2 * n$

$D_{ARSA} = f(A) = A$

FIG.3a.



$R = S = S^{d}(M)$

$Q1 = S * S / n$

$Q2 = S(S * S - Q1 * n)/n$

$D_{SRSA} = S(S * S - Q1 * n) - Q2 * n$

$D_{SRSA} = f(M)$.

FIG.3b.